IoT
Security Foundation

Vulnerability Disclosure

Release 2.0, September 2021

Best Practice Guidelines

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org/

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high-quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document

- Jeff Day, BT plc
- Professor Paul Kearney, Birmingham City University
- John Moor, IoT Security Foundation
- Richard Marshall, Xitex Ltd
- Andrew Bott, Secure Thingz Ltd
- Ian Poyner, IoT Security Foundation

Peer Reviewers:

- Professor Mark Zwolinski
- Çağatay Büyüktopçu

Plus silent others – you know who you are!

Contents

1 Introduction

1.1 Overview

It is vital to the commercial interests of providers of Internet of Things (IoT) products and solutions and to the security of their customers, that vulnerabilities are discovered and remediated as soon as possible. Third party security researchers are a valuable adjunct to a provider's internal resources in addressing this goal. To ensure effective co-operation and maintain good relations with external security researchers, it is important for providers to define and communicate vulnerability disclosure processes that not only describe how they would like vulnerabilities to be reported confidentially to them, but also set expectations as to how they will process and act upon such reports. This process should include provision of feedback to the discovering researcher, and the public announcement of the security vulnerability, usually after the release of a software patch, hardware fix, or other remediation.

The ETSI 303 645 standard [4], which lays down baseline security requirements for the consumer IoT, includes requirement 5.2, to *"Implement a means to manage reports of vulnerabilities"*. This states that *"The manufacturer shall make a vulnerability disclosure policy publicly available."*, adding that *"A vulnerability disclosure policy clearly specifies the process through which security researchers and others are able to report issues."*

The following document provides manufacturers, integrators, distributors, and retailers of IoT products and services with a set of guidelines for handling the disclosure of security vulnerabilities, based on best practice and international standards.

The IoT Security Foundation have a "Manage Vulnerability Reports" webinar series to complement this document.

1.2 Scope

This document presents best practice guidelines for a vulnerability disclosure process, recommended for adoption by IoT solution providers, device vendors and service providers.

It is based on international standards **ISO/IEC 29147:2018, Information technology -- Security techniques -- Vulnerability disclosure** [1] and **ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes** [2]. These ISO documents cover the vulnerability disclosure subject in fine detail and are available for purchase on the ISO website. NIST SP800-216 '*Recommendations for Federal Vulnerability Disclosure Guidelines*' [5] is an example of guidelines based upon these two ISO/IEC standards.

The following terms are used in alignment with ISO/IEC 29147:2018 [1] and ISO/IEC 30111:2019 [2]:

- **Vendor** – "The individual or organization that is responsible for remediating vulnerabilities" - Typically the developer, maintainer, producer, manufacturer, supplier, installer, or provider of a product or service.

- **Reporter** – “An individual or organization that notifies a vendor of a potential vulnerability” – Typically individuals, organizations, amateurs or hobbyists, professionals, end-users, security researchers, vendors, governments, or other interested party.

NOTE ON DATA PROTECTION: This document does not address the management of any data breach which may have resulted from the exploitation of a security vulnerability. An organisation’s responsibilities regarding this are usually determined by prevailing legislation and government regulations (particularly regarding individuals’ personal data) in the territories and/or industry sectors in which they operate. An organisation must ensure it is fully aware of, and in compliance with, all applicable data protection requirements.

2 Vulnerability Disclosure Policy

A Vulnerability Disclosure Policy (Policy) is a publicly available document, typically accessed via the Vendor's reporting web page. It is the Vendor's statement as to how they will handle any vulnerability report passed to them. There is no set text for such a Policy, but there are many examples available online that can help as a starting point. The NCSC toolkit [3] and ISO 29147:2018 [1] both provide sample policy text, and numerous well known technology companies have published their own policies.

There are however certain key points to consider when developing a Vulnerability Disclosure Policy:

- Use plain language. Avoid complicated or specialist terminology.

- A draft Policy is required to direct the establishment of internal processes and resources. The processes and resources need to be fully tested so that it is clear how the overall system (reporting->mitigation) will operate. Only once the processes are verified should the final Policy be published.

- Always get approval from the legal team before publishing.

- Clearly define the scope of what is and isn't covered by the Policy.

- Explain the appropriate means of communication and Vendor contact details, e.g. the designated reporting web page, email address, encryption requirements etc. (as required).

- Explain what information is needed as part of any report submission.

- Define the time scales involved. Be realistic so the Vendor always has a fair chance of meeting their own targets. However also consider that the Reporter will be eager to see the issue is being resolved; overly-long-time scales may make the Reporter feel that the Vendor lacks urgency in the matter. Be this a right or wrong assessment, it doesn't help to set the relationship off on a good footing.

- Explain what kind of reporting structure will be in place, i.e., how the Reporter will be kept updated by the Vendor, and what happens once the issue has been fully assessed. For example, the Policy may say that after initial confirmation of receipt, the Vendor aims to provide initial feedback to the Reporter to advise on their findings; what happens thereafter may depend on what is found.

- Also state in the Policy that if the Vendor has to refer out to a 3rd party (e.g., if the product uses third-party proprietary code) then the time required for assessment and development of mitigations may need to be extended. The additional time will depend on the priority given to the issue by the 3rd party, which is largely beyond the control of the Vendor. In such circumstances, a reliable estimate of completion time may be difficult to obtain.

- Bear in mind vulnerability reports may be generated from inside the Vendor's company. Any Policy should either apply to both public Reporters and internal Reporters, or a separate internal Policy will need to be written. It would be expected that the internal Policy version should align closely with the public Policy version.

- The Policy should also make it clear what actions a Reporter must refrain from when hunting for vulnerabilities, such as conducting unapproved denial of service attacks, load tests, social engineering, or other undesirable activities.

- Reporters should also be reminded that any activities they undertake must always remain within legal boundaries.

- Given all the above points, do keep in mind that the Reporter is generally trying to do the right thing by making the Vendor aware of an issue with their product. The Vendor should aim to be respectful of the Reporter's intent, work with the Reporter and behave in a fair and professional manner. This approach should be reflected in the wording of the Policy, whereby the overall process operates with the Vendor and Reporter working together in a coordinated fashion. This approach will promote positive outcomes for everyone.

- To support positive engagement with Reporters, the Policy should also state how, and under what circumstances, the Reporter will be recognised for their contribution. Typically, this could be thanking the Reporter within an Advisory notice published as part of any vulnerability mitigation activities, and/or perhaps posting their name on the original reporting page. However, such recognition must only be done with the Reporter's written agreement and with clarification on how they want to be identified, e.g., Reporter's Name + Employer Name, or Reporter's Name + Twitter handle etc., whatever they reasonably request.

- 'Bug Bounties' – A Policy must make it clear whether or not the Vendor offers financial (or other kinds of) rewards for identifying vulnerabilities. If a Vendor decides they do want to offer financial incentives, they should consider the following issues before committing to such an approach:

    - A financial incentive is likely to encourage more vulnerability reports than may happen if no rewards were offered. This creates a greater workload on the whole vulnerability disclosure management pipeline. It may also create a need to triage the priority of each disclosure, with the added risk of a Reporter whose vulnerability is deemed 'low priority' deciding to go public.
    - With potential financial rewards on offer, there is an increased chance some Reporters may have fraudulent intent in mind. At best this wastes a Vendor's time & resources, at worst it could defraud the Vendor.
    - The Vendor must determine a payment framework. How will that work? Will there be just one fixed payment, regardless of the type of vulnerability reported? Will there be a sliding scale of payment, and if so, then what measure is used to position a given vulnerability on the payment scale? Reporters may not be happy with their reward value if they feel their findings merit a higher reward. If several significantly high-risk vulnerabilities are identified by Reporters, rated as per the Policy as deserving high value rewards, what financial impact will this have on the Vendor company's finances?
    - An unscrupulous developer who works for the Vendor may decide to write vulnerabilities into a product's source code. Subsequently they (or an accomplice) could then 'discover' a vulnerability and claim the bounty. Irrespective of this fraudulent behaviour, isn't a developer who discovers a vulnerability in their employer's code just doing their job, which they are getting paid to resolve/avoid

anyway, so are they truly entitled to a bounty reward? Has this kind of scenario been covered by a clear clause in the Policy around employees/contractors and their bug bounty entitlements?

- What happens if several Reporters report the same vulnerability? Will they share the reward? Will it go to the first to report it?

These and many other possible issues may make the reality of offering bug bounties problematic for some organisations. Bounties are not necessarily the wrong thing to do, however a Vendor should consider the implications carefully, and consult their legal and finance teams, before committing to offering financial rewards.

3 Vulnerability Disclosure Process Guidelines

Figure 1 shows a high-level process Vendors can follow to manage vulnerability disclosure. The Vendor's process runs down the middle of the flowchart, with inputs & outputs to each side. Ideally, communication with the Reporter should be an ongoing dialogue throughout the process.

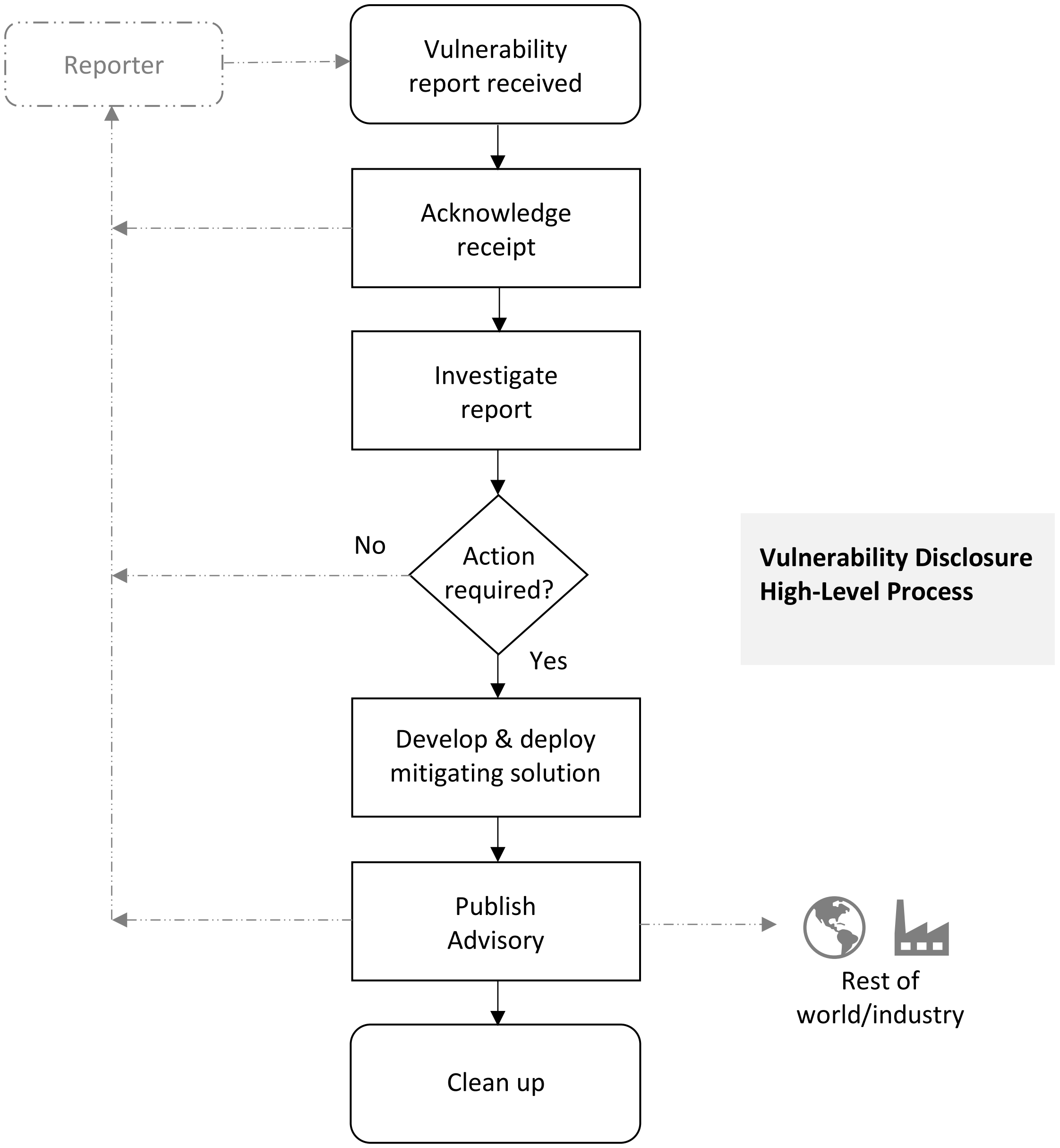

Figure 1

It is up to each individual Vendor to decide exactly what process to adopt, but it is important to be clear about the process in public materials, websites and in communications with Reporters, to align expectations.

A senior executive should own the process and have overall responsibility within the company for ensuring the process is appropriately resourced and implemented.

The rest of this document looks at the issues involved at each stage of this process.

3.1 Vulnerability Report Received

3.1.1 Publicising the point of contact

It is essential that Reporters of vulnerabilities can be readily channelled to the right point of contact within a Vendor's organisation, so it is imperative to make this information easy to find on the Vendor's web site. The Vendor should place a web page giving the contact instructions in a standard, well-known location. Two conventions are explained below:

1. https://www.companydomain/security. E.g. Reporters can contact the IoT Security Foundation at https://www.iotsecurityfoundation.org/security if they want to report some kind of vulnerability issue with any of the Foundation's products or services.
2. The UK's National Cyber Security Centre (NCSC) recommend using the **security.txt** convention. This is a proposed internet standard whereby machine-parsable information about the vulnerability disclosure process is provided in the location https:/www.companydomain/.well-known/security.txt. Further details can be found at https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit and https://securitytxt.org/

A link to the vulnerability reporting page should also be included in the web site's "Contact Us" page.

Details of any vulnerability should be handled securely at least until a mitigating solution is available. Therefore, Reporters should be offered a secure mechanism for reporting their findings. Typically, this could be via a web form submitted over an HTTPS connection. Alternatively, a Reporter may wish to remain anonymous or use a pseudonym and have their own preferred method of secure communication (see section 3.1.3 on 'Capturing Vulnerability Details'); in this situation the Vendor should remain flexible and accommodate the Reporter if it does not compromise the Vendor. Keep in mind that if alternative, less secure communication options are provided, these may increase the risk of early exposure of the new vulnerability.

3.1.2 Web Page Text

As a minimum the page should state, or provide a link to, the Vendor's full Vulnerability Disclosure Policy, and a secure means to submit details about the vulnerability the Reporter has found.

It is recommended that the amount of text on the front page of a vulnerability reporting site be kept to a minimum. If a Reporter is faced with pages of block text, they may be put off and not bother to make the report, which is counterproductive.

3.1.3 Capturing Vulnerability Details

There are two issues to consider at this stage: (1) the Reporter themselves; (2) what they must report.

Some Reporters will be keen to give you their name and full contact details, whereas others may be reticent about revealing their identity, especially if their journey to finding the vulnerability bordered on the edge of legality. Either approach needs to be respectfully maintained, as any breakdown in trust between the Reporter and Vendor will only hinder information gathering. Such a break down in trust may lead to a Reporter taking unilateral action. This could result in early public exposure of details of the vulnerability, or perhaps negative reports in the media, unjustified or not, with consequential impact to brand image, loss of sales etc. as possible outcomes. It is therefore best to try and maintain a trusted relationship with a Reporter as far as possible.

As previously stated, aim to collect information about the vulnerability via a secure channel. Exactly what information is required from the Reporter will depend on the nature of the vulnerability being reported. However, some basic details will always be required, typically:

- Reporter's name (or self-declared pseudonym)
- Reporter's contact details: Email, phone number(s), Twitter handle, Facebook, etc. (but they may not offer any these)
- Reporter's reference number (if applicable)
- Positive confirmation from the Reporter they have read & understood the Vendor's Vulnerability Disclosure Policy
- Name of affected product/service, plus specific version number, model number, serial number etc.
- Any Proof of Concept (PoC) setup details
- Description of steps to reproduce the issue
- Perceived impact and severity if the vulnerability were to be exploited
- Any perceived impact on other products, services, vendors etc.
- Any intended further actions by the Reporter, their expectations from the Vendor etc.
- Other relevant information

The Reporter may wish only to reveal limited information at this stage. As the dialogue between the Reporter and Vendor progresses, it is often possible to gain further details of the exact nature of the vulnerability that the Reporter has discovered.

3.1.3.1 Information Gathering Options – Web Form

Offering a web form to complete allows the Vendor to collect the above information from the Reporter in a structured and uniform way. This simplifies the task of capturing and processing reports, but requires web forms to be designed, developed, and maintained. A well-designed form will help the average user who has stumbled across something they think needs reporting to provide the required information as best they can. However, a badly designed form with poorly worded questions can be confusing, deterring reporting and resulting in poor quality data being captured.

3.1.3.2 Information Gathering Options – Encrypted Email

An alternative mechanism for providing vulnerability details is encrypted email. More technically knowledgeable Reporters may be happy to report via an email encrypted with the Vendor's Open PGP public key. If offering this option, the Vendor's public PGP key should be provided on the reporting page, along with a link to the Open PGP website for further information.

The reporting page should also state the email address the Reporter should send to. Within the industry the address would typically be expected to be one of the following:

- security-alert@*companydomain*.com
- security@*companydomain*.com

- psirt@*companydomain*.com (Product Security Incident Response Team)
- csirt@*companydomain*.com (Computer Security Incident Response Team)

3.1.4 Initial Report Handling

Once a report has been submitted, the receiving system should immediately return an automated response to acknowledge the Vendor has successfully received the report. Once they receive the response, the Reporter will consider that the notification to the Vendor has taken place and will be expecting prompt action. It is therefore important the incoming report is immediately flagged to a specific incident response team within the Vendor organisation for attention.

The Vendor's incident response team must always have sufficient resources to ensure:

A) The report is logged and documented, and passed on as soon as possible to the relevant party to investigate

B) An acknowledgement is sent back to the Reporter to advise the issue is now being investigated

C) Internal and customer communications are managed effectively.

The initial report handling stage should not come to a halt just because someone goes on leave for two weeks. Failing to meet the Vendor's first response target as defined in their own Policy will not start the process well in the eyes of the Reporter (see other comments around maintaining trust with Reporters).

3.1.5 Communicating with the Reporter

All communications with the Reporter must be professional, consistent and in line with the published Vulnerability Disclosure Policy. Reporters may have a wide variety of backgrounds and expectations; they may be, for example, hobbyists unused to business processes, academics who desire the freedom to publish research, or professional consultants building a reputation for expertise in finding security problems. It is important, in communication with Reporters, that due consideration and recognition is given to the effort they have devoted to researching the particular security problem. Their motivation and expectations may well differ from the Vendor's, so it is imperative they are given enough room to work with the Vendor and that a constructive, understanding tone is always adopted, even if their actions may seem inappropriate in the Vendor's business context.

Sometimes a Reporter might stipulate a time scale by which the Vendor should respond in some way, after which the vulnerability will be publicly disclosed. Usually, this statement is made to encourage less engaged Vendors to take timely action, or the Reporter wishes to present it at a major conference of cyber researchers (e.g.: DEF CON). Responsible Vendors will naturally engage in addressing a reported vulnerability in a timely fashion, but sometimes for good reasons these time scales won't match the expectations of a Reporter. Rather than take affront and refuse to accept an imposed time limit, Vendors are encouraged to have an open discussion with Reporters and reach agreement on how a solution can best be delivered. Most Reporters will be accommodating to honest and realistic responses in this matter.

There may be many people involved in investigating a report, therefore it is recommended to have just one single communications point within the Vendor's process. This will help ensure all communications are consistent, minimise the risk of messages getting lost, help avoid confusion for the Reporter and enable end to end traceability of the overall report handling.

3.1.6 Report Ownership and Communication

Every report received should have an owner who has the consequential responsibility for ensuring standards are maintained in terms of communications and adherence to published time scales. The incident response team should have overall ownership for every report received, and for ensuring continuity in the absence of the nominated owner. It then becomes their responsibility to handle all communications with the Reporter and ensure every report is processed through to conclusion in accordance with the published Policy. This team don't have to do the actual investigation and any subsequent technical work, but they must ensure the report is tracked and addressed in accordance with the Policy (communications, timing etc.).

Vendor communications, both internally and to its customers, are also important, for example:

- Briefing Senior executives on the resolution of the vulnerability discovery.
- Ensuring consistent messaging on the progress and vulnerability details across the Vendor's organization and in any customer communications.

The content of vulnerability communications should be provided by and/or authorized by the incident response team. This is to ensure consistent and accurate communication with audiences who are unlikely to have an in depth understanding of the nuances of the security vulnerability disclosure. The PR/media communications and legal teams may also be involved prior to public disclosure. This can be crucial in supporting business development teams in their management of customer relations.

3.2 Acknowledgement of Report Submission

Once the incident response team have passed the report on to be investigated, they should then send an acknowledgement to the Reporter advising their report is now under initial investigation. This gives the Reporter some comfort that a real person is now dealing with their report.

The acknowledgement should at least include the following:

- Thank the Reporter for submitting the report.
- Provide a link to the Vendor's Vulnerability Disclosure Policy.
- Provide contact details to which the Reporter can make any further communications with the Vendor's incident response team.
- Advise what will happen next and when.

3.3 Investigation of the Report

The incident response team should send the report to the responsible party in the Vendor's organisation to verify whether the vulnerability is real or not. It must be clear in the handover documentation what the response time scales are, as defined in the published Policy.

The triage activity will be somewhat specific to the nature of the Vendor's business, but the following points should be noted:

- Careful attention should be paid to any set up requirements given by the Reporter and other points of note they may have indicated to reproduce the problem.
- Monitor progress against the response time scale. Any significant anticipated or real deviation from this should be flagged back to the incident response team as soon as possible. A decision can then be made to consider what communication is necessary with the Reporter.
- If the reported vulnerability cannot be reproduced by the investigating team, seek further communication with the Reporter (via the incident response team) and work with them collaboratively to try and identify the underlying problem.
- If the vulnerability is deemed to be real, the Vendor will, among other things, need to consider the following: Is the vulnerability within the Vendor's own product or actually within a contributing 3rd party's product (e.g. 3rd party software library); is this a duplicate of an already known vulnerability; what other products may be impacted; what is the severity of the vulnerability; what might be the cost of mitigation; is the product still supported; what is the priority of remediation; and is it actually a security issue rather than a functional issue ?
- The outcome of the initial investigation must be reported back to the incident response team as soon as possible. The decision(s) of the investigation must be clear and unambiguous.

3.4 Action Required?

There are two potential outcomes here, either the Vendor decides action is required, or it is not required.

3.4.1 Action is not required

The Vendor may decide action is not required for either of two reasons:

- The Vendor is satisfied the vulnerability is not real

  or

- The Vendor has made a business decision that although the vulnerability is real, they will not be taking action because of XYZ reason.

In real world scenarios, not all vulnerabilities will be considered urgent or even worthy of a fix by a Vendor. There may be good reasons not to address a known vulnerability – for example if it is judged to be minor or of low/no impact. Such a decision must not be taken lightly however and should be considered as an exceptional approach only. Not mitigating a vulnerability may result in real compromises occurring, with a consequential impact (to varying degrees) on the Vendor's products and services, third-party equipment, customers' privacy, convenience or networks, the Internet, the Vendor's brand image, future sales etc. Someone of appropriate authority/responsibility within the Vendor organisation must be made clearly aware of the potential impact of no action and be prepared to sign off to accept such a risk on behalf of the business. If in doubt, fix the vulnerability.

3.4.2 Action is required

If the Vendor determines the vulnerability is real, they must now, in coordination with the incident response team, move the process on to the next stage of developing and deploying a mitigating solution.

3.4.3 Communication with the Reporter

Whatever action the Vendor decides to adopt, they should communicate with the Reporter at this stage to appraise them of the outcome of the initial investigation. The Reporter should, of course, be thanked for their interest, help and support with the report and informed of what will happen next (if anything), in accordance with the Policy.

Where the decision has been made to take no action, the Vendor must be very clear on why that is. If it believes there is no vulnerability to address, this must be clearly explained in the communications with the Reporter, outlining the reasoning behind this outcome. The investigation team may have already engaged with the Reporter to help diagnose the issue, in which case the outcome of no vulnerability shouldn't come as a surprise. If, however, this is the first communication back to the Reporter since receipt acknowledgement, the Reporter should receive a clear explanation of the findings to help them understand why their submission resulted in no action.

If the Vendor decides to take no action against a real vulnerability, they need to provide the Reporter with a clear explanation as to why the Vendor is taking this stance. Keep in mind the Reporter's values are more likely to align with concerns about the impact on the user and may not align with those of the Vendor.

3.4.4 Resolving Conflict

A Vendor should be prepared for significant pushback from the Reporter to the news 'their' vulnerability won't be resolved. The Reporter will have their own views on the issue, which may well not align with that of the Vendor. If a Reporter doesn't get the answer they want to hear (be that right or wrong), their reaction could be anything from resigned acceptance to significant indignation. In the latter case, action could take all forms, from harassment, to negative messages through the press and social media or even legal action. Therefore, such a decision cannot be taken lightly, as previously discussed.

With good management, a message from the Vendor delivered clearly and professionally, with a clear and justifiable rationale, is likely to be received with the good grace in which it was intended.

If the relationship with the Reporter does unfortunately break down and somehow impacts progress of the process, the Vendor should:

- Leave the process only after exhausting reasonable efforts to resolve the disagreement
- Leave the process only after providing notice to the Reporter
- Aim to resume the process once the disagreement is resolved and the Reporter is re-engaged

3.5 Develop & Deploy Mitigating Solution

Quite how a deliverable solution to a vulnerability is achieved by a Vendor is very much specific to that company and the product or service involved and falls out of scope of these guidelines. However, the following points should be considered:

- If delivery dates are expected to slip in relation to what may have been agreed with the Reporter, the Reporter should be informed of the situation to help maintain engagement and goodwill.

- Depending on the Reporter's skills and the nature of their relationship with the Vendor, a Vendor may wish to include the Reporter in testing of a pre-release version of the fix. This often maintains the goodwill of the Reporter, who in turn will be checking the fix against the original source of the identified problem.

- A software fix could be released as part of the Vendor's standard patch/update delivery cycle, or perhaps made available as a one-off out-of-band release. Various circumstances will dictate which option to choose, such as timing of the Vendor's standard patch/update cycle or the level of risk posed by the vulnerability.

- Also consider whether information about the vulnerability should be passed on to other departments within the Vendor organisation, particularly customer facing ones. It should be kept in mind the conflicting considerations of sharing the details of a vulnerability too widely. Where it is necessary to share vulnerability details with customers ahead of public advisories, the incident response team should be the sole source of the detail for such customer communication.

3.6 Publish Advisory

The organisation should have controlled disclosure channels for issuing security advisories to users and relevant stakeholders, and to inform them of the mitigating solution (if available). It is advisable to contact all known users of the product before publicly disseminating the Advisory. This provides opportunity to mitigate the impact if a fix is not available (replace or isolate a device from any threat) or apply the fix before the vulnerability becomes public knowledge. Consideration will need to be given to how much lead time might be required to deploy the fix– especially if it is not automated. Stakeholders may also include anti-malware vendors and service providers.

To support this early notification, the Vendor could have a mailing list via which alerts can be sent to subscribers (registered customers), providing details of the fix and where to find further information, e.g., a private download site for the signed software patch. Depending how the product is purchased, the Vendor may be able to use existing customer contact details as another route to notify customers. It's recommended Vendors digitally sign any Advisory to registered customers to demonstrate authenticity of the communication.

Typically, a Vendor will have a web site where they publicly list details of upgrades, new features and advisories to their products, along with the relevant software downloads (which should be digitally signed, along with published hash values for each download package – see IoTSF Best Practice Guides for more details on this). A new Advisory should only be listed here once registered customers have had a reasonable opportunity to test and deploy the patch in advance within their own networks. The Vendor may provide help and assistance to users over social media channels and user forum communities.

The Vendor should consider how they will publicly recognise the contribution from the Reporter. It's up to the Vendor to decide how they do this, but it should be done in agreement with the Reporter. An example might be a line in the Advisory such as the following: "*We would like to thank <Reporter's name> of <Reporter's employer> for his/her valuable contribution in identifying this vulnerability and support while we developed the solution.*".

3.7 Clean Up

At some point the incident response team will need to close the vulnerability report. The Vendor will need to decide at which stage of the process this should happen. Keep in mind that software patches don't always behave as planned, especially if the fix was rolled out with some urgency. It's not uncommon to come across unexpected incompatibility issues or unforeseen side effects. Thus, it may be prudent as a standard approach to keep the report open for 3 months (as an example) after public release of the Advisory to ensure unexpected issues get included in the vulnerability management reporting.

3.7.1 Post Incident Review (PIR)

It is recommended that a PIR is held with representatives from involved stakeholders about two weeks after the Advisory is publicly published, to review how the process was handled. This meeting can consider and record lessons learned and generate any necessary actions to help improve how the vulnerability management process operates in the future.

Careful analysis should be undertaken of the root cause(s) of the vulnerability and what other product families may also be impacted. There may have been an initial assessment during the development of the mitigation solution, but a more complete analysis should be completed with the full details now available.

4 References and Abbreviations

4.1 Organisations

The following organisations are referenced in this document:

ETSI	European Telecommunications Standards Institute
IoTSF	Internet of Things Security Foundation
NCSC	UK National Cyber Security Centre
NIST	National Institute of Standards and Technology

4.2 References

The following references are used in this document:

1. ISO/IEC 29147:2018, Information technology -- Security techniques -- Vulnerability disclosure
2. ISO/IEC 30111:2019, Information technology -- Security techniques -- Vulnerability handling processes
3. National Cyber Security Centre (NCSC) Vulnerability Disclosure Toolkit
4. ETSI 303 645 v2.1.1 (2020-06)
5. NIST SP 800-216(Draft)

4.3 Definitions and Abbreviations

For the purposes of the present document, the following abbreviations apply:

(Security) Advisory	An announcement or bulletin that informs users about a vulnerability in a product or service, usually including instructions on how to remediate the vulnerability
CSIRT	Computer Security Incident Response Team
Data Breach	Any incident that results in unauthorized access to data, networks, devices or services
IoT	Internet of Things
ISO	International Organization for Standardization
PIR	Post Incident Review
PSIRT	Product Security Incident Response Team
Reporter	An individual or organization that notifies a Vendor of a potential vulnerability (ISO 29147 definition)

Vendor	The individual or organization responsible for remediating vulnerabilities, typically the developer, maintainer, producer, manufacturer, supplier, installer, or provider of a product or service (ISO 29147 definition)
Vulnerability	A weakness in a system that can be exploited to compromise security
Vulnerability Disclosure Policy	A Vendor’s statement as to how they will handle any vulnerability report passed to them

IoT Security Foundation

www.iotsecurityfoundation.org